UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/577,448	04/27/2006	Masao Nonaka	2006_0611A	4794

52349 7590 08/03/2009

WENDEROTH, LIND & PONACK L.L.P.
1030 15th Street, N.W.
Suite 400 East
Washington, DC 20005-1503

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
08/03/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/577,448	NONAKA ET AL.	
	Examiner	Art Unit	
	JEFFREY D. POPHAM	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 April 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 April 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *20060427*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Remarks

Claims 1-39 are pending.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

1. Claims 29-33 and 37-39 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Each of these claims is directed to "A program to be used...", "the program comprising:" steps. This program is not, however, stored on any computer readable storage medium, nor is it executed by any device/processor. It is noted that claims 33 and 37-39 each fix the computer readable storage medium aspect of the 101 issue of the corresponding claims above. For example, claim 33 adds a computer readable recording medium on which a program according to claim 29 is recorded. If this were to be added to claim 29 itself, there would be a computer readable recording medium (defined in the specification as being a ROM or CD-ROM, for example) upon which the program is recorded. Upon also adding in that the program is executed by the device referred to in the preamble (such as claim 29 referring to the content distribution server), the claim would be statutory. However, without the program of claim 29 being stored on a computer readable storage medium and executed by a device/processor, the claim is not statutory. The same analysis is made for each of claims 30-32. Claims 33 and 37-39 are rejected for like reasons with respect to the execution aspects.

Claim Objections

2. Claims 2, 3, 5, 8, 11-16, 23, 25, 32, and 39 are objected to because of the following informalities:

- The third limitation of claim 2 reads "selecting a terminal node in the tree structure, the terminal node being (i) a node that belongs to the nth level, and (ii) a node that belongs to the jth level (j is a natural number from 1 to n-1) and is not connected by lines with any nodes belonging to the j+1th through the nth level". There are multiple issues here. First noted is that a single terminal node cannot be both on the nth level as well as on the jth level. Each terminal node has 1 instance on the tree, as a leaf of the tree. The Examiner has construed the "and" before (ii) as "or" as that appears to be the only proper interpretation of this limitation with respect to the claim (that each terminal node is either at a position corresponding to (i) or (ii) on the tree). The second issue is that it is unclear what "not connected by lines" is supposed to mean. The Examiner has construed this as meaning that the node is a leaf on the tree and, therefore, has no descendants. This must be clarified by amendment in order to properly define the scope of the claim. Claims 11, 13, 23, and 32 also have this issue, and claims 3, 5, 12, 14-16, and 39 also have the same issue by dependency.

- Claim 8 refers to “the encrypted key group selection unit”, which has been construed as “the encryption key group selection unit” for proper antecedent basis.
- The second to last limitation of claim 25 recites "receiving the content output apparatus identifier from outside via the network". It is unclear what "from outside" means. This has been interpreted, in its broadest form, to be anything outside the key issuing center.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 11-16, 32, and 39 are rejected under 35 U.S.C. 102(b) as being anticipated by Nakano (WO 02/078419 A2).

Regarding Claim 11,

Nakano discloses a key assignment method for assigning a node decryption key for obtaining a content decryption key to each of content output apparatuses connected with a content distribution server via a network, the content distribution server distributing a content encrypted using a content encryption key, the content output apparatus receiving the

encrypted content and decrypting the encrypted content using the content decryption key, and the method having one or more tree structures, in each of which a plurality of content output apparatuses serve as nodes, and comprising:

Classifying the nodes into a plurality of levels from a 0^{th} level through an nth level (n is 1 or a larger natural number) (Figure 4; and Page 33, lines 7-17; showing a 4-ary tree);

Setting one or more pairs of node encryption keys and corresponding node decryption keys for all the nodes that make up the tree structure (Page 38, lines 10-15);

Selecting a terminal node in the tree structure, the terminal node being (i) a node that belongs to the nth level or (ii) a node that belongs to the jth level (j is a natural number from 1 to n-1) and is not connected by lines with any nodes belonging to the j+1th through the nth level (Figure 4; Page 33, lines 7-17; and Page 35, line 26 to Page 36, line 3);

Associating one of the terminal nodes with the content output apparatus to which the content is to be distributed, and assigning, to the output apparatus, a set of the node decryption keys which are set for respective nodes belonging to a relevant node set which is relevant to the associated terminal node, as a node decryption key group (Figure 11; and Page 42, line 24 to Page 43, line 25); and

Distributing the node decryption key group to the content output apparatus (Figures 3 and 22; and Page 34, lines 4-16; such distribution being done through the manufacturing system as an intermediary before reaching the apparatus).

It is briefly noted that the Examiner first rejected claims 1-10, and that some of the pertinent discussion with respect to the above-cited portions of Nakano will be thoroughly discussed below.

Regarding Claim 32,

Claim 32 is a program claim that corresponds to method claim 11 and is rejected for the same reasons.

Regarding Claim 39,

Claim 39 is a computer readable recording medium claim that corresponds to method claim 11 and is rejected for the same reasons.

Regarding Claim 12,

Nakano discloses that the relevant node set includes at least one terminal node, a parent node of the terminal node and a series of parent nodes of the parent node (Figure 11; and Page 42, line 24 to Page 43, line 25; showing the node set including 3-1K corresponding to the terminal, as well as 7 keys for each parent. 2-1 being the node's direct parent, 1-1 being the parent's parent, and 0-1 being the parent of the parent's parent, also referred to as root); and

In the assigning, the node decryption keys which are set for the nodes belonging to the relevant node set are assigned as the node decryption key group (Figure 11; and Page 42, line 24 to Page 43, line 25).

Regarding Claim 13,

Nakano discloses that a node belonging to the ith level (i is a natural number from 1 to n) in the tree structure is connected by a line to a parent node that is one of nodes belonging to the 0th level to the i-1th level (Figures 14-15); and

In the assigning, the node decryption keys corresponding to the parent nodes connected by lines are assigned as the node decryption key group (Figure 11; and Page 42, line 24 to Page 43, line 25).

Regarding Claim 14,

Nakano discloses that only one node belongs to the 0^{th} level (Figures 14-15; Level 0 including solely the root node, also referred to with the node designation/identification 0-1).

Regarding Claim 15,

Nakano discloses setting the node encryption keys for all the nodes as a node encryption key group corresponding to the node decryption key group assigned in the assigning (Page 38, lines 10-15; showing key sets or pairs for each node, comprising an encryption key associated with a decryption key).

Regarding Claim 16,

Nakano discloses that the tree structure in the key assignment method is an N-ary tree (N is 2 or a larger natural number) (Figures 14-15; showing a 4-ary tree).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-10, 29, 33, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakano in view of Lao (U.S. Patent 7,343,324).

Regarding Claim 1,

Nakano discloses a content distribution server that encrypts a content and distributes the encrypted content to content output apparatuses connected to the content distribution server via a network, each of the content output apparatuses decrypting the encrypted content and outputting the decrypted content, the content distribution server (encryption device, for example) comprising:

A key information storage unit operable to hold a node encryption key group that is a set of node encryption keys which are previously assigned to the content output apparatuses using a predetermined key

assignment method (Page 29, lines 8-22; encryption key group storage unit storing keys and key designation information received from key setting system);

An encryption key group selection unit operable to select, from among the node encryption key group, at least one node encryption key as a selected node encryption key group (Page 22, line 8 to Page 23, line 11; deciding and selecting keys to be used);

A content decryption key selection unit operable to generate an encrypted content decryption key group that includes at least one encrypted content decryption key obtained by encrypting a previously given content decryption key using the at least one node encryption key in the selected node encryption key group (Page 29, lines 4-7 and 23-27; key encryption unit encrypted the generated content key using each stored/selected encryption key);

An encryption unit operable to encrypt the content using a content encryption key which is previously given as a pair with the content decryption key (Page 29, line 28 to Page 30, line 3; content encryption unit encrypting the content with the content key; one will note that the instant application states that "A content encryption key CEK and a corresponding content decryption key may have the same value" (Page 42, lines 14-15). Therefore, even in embodiments of Nakano in which the keys are

symmetric, the symmetric key clearly reads on the combination of encryption key and decryption key); and

A transmission unit operable to distribute the encrypted content and the encrypted content decryption key group to the content output apparatuses (Page 30, lines 4-10; and Page 74, line 23 to Page 75, line 14; the output unit employing transmission across transmission paths);

But does not explicitly disclose a content receiving unit operable to receive a content via the network.

Lao, however, discloses a content receiving unit operable to receive a content via the network (Figure 7; Column 1, lines 8-12; Column 6, lines 31-36; Column 7, lines 63-67; and Column 9, lines 61-67; the distributor receiving content over a network). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the content publishing system of Lao into the data protection system of Nakano in order to allow the creators of content to specify the rights that may be allowed for a particular piece of content before allowing the content to be distributed, thereby ensuring proper control for content creators.

Regarding Claim 29,

Claim 29 is a program claim that corresponds to server claim 1 and is rejected for the same reasons.

Regarding Claim 33,

Claim 33 is a computer readable recording medium claim that corresponds to server claim 1 and is rejected for the same reasons.

Regarding Claim 34,

Claim 34 is a method claim that corresponds to server claim 1 and is rejected for the same reasons.

Regarding Claim 2,

Nakano as modified by Lao discloses the server of claim 1, in addition, Nakano discloses that the key assignment method has a tree structure in which a plurality of content output apparatuses serve as nodes, and includes:

Classifying the nodes into a plurality of levels from a 0^{th} level through an nth level (n is 1 or a larger natural number) (Figure 4; and Page 33, lines 7-17; showing a 4-ary tree);

Selecting a terminal node in the tree structure, the terminal node being (i) a node that belongs to the nth level, or (ii) a node that belongs to the jth level (j is a natural number from 1 to n-1) and is not connected by lines with any nodes belonging to the j+1th through the nth level (Figure 4; Page 33, lines 7-17; and Page 35, line 26 to Page 36, line 3; showing terminals as being leaves, as well as the possibility that not every lowest-level node will be associated with a terminal, therefore, providing for leaf nodes that are not on the lowest level); and

The encryption key group selection unit selects the selected node encryption key group so that the selected node encryption key group includes at least a node encryption key that is set for a terminal node and a node encryption key that is set for a node other than the terminal node (Figure 4; and Page 33, lines 7-17; showing assignment of keys to nodes of the tree).

Regarding Claim 3,

Nakano as modified by Lao discloses the server of claim 2, in addition, Nakano discloses that the tree structure in the key assignment method is an N-ary tree (N is 2 or a larger natural number) (Figure 4; showing a 4-ary tree).

Regarding Claim 4,

Nakano as modified by Lao discloses the server of claim 1, in addition, Nakano discloses a content key generation unit operable to newly generate at least one pair of a content encryption key and a corresponding content decryption key which is different from at least one pair of a content encryption key which is previously used for encrypting a content and a corresponding content decryption key, in the case where the content receiving unit receives a new content (Page 29, lines 4-7; and Page 29, line 23 to Page 30, line 3; randomly generating the content key).

Regarding Claim 5,

Nakano as modified by Lao discloses the server of claim 2, in addition, Nakano discloses that the encryption key group selection unit newly selects a selected node encryption key group including a node encryption key that is set for another terminal node than a previously selected terminal node, in the case of receiving a new content via the content receiving unit (Figures 14 and 15; Page 22, line 8 to Page 23, line 11; Page 48, line 24 to Page 49, line 3; and Page 51, lines 9-13; showing that content may, at first, be sent using the key 0-1K0000, which is held by all decryption devices; the invalidation of device 1; and the use of keys 0-1K1000, 1-1K1000, and 2-1K1000 in encrypting keys for later provided content, such that device 1 cannot access the content, since it has no keys that can be used to decrypt the content key).

Regarding Claim 6,

Nakano as modified by Lao discloses the server of claim 1, in addition, Nakano discloses a key selection information storage unit operable to hold a plurality of key selection information which are used for selecting the node encryption key included in the node encryption key group (Page 29, lines 8-22; storage of key designation information);

Wherein the encryption key group selection unit selects the selected node encryption key group based on the key selection information (Page 22, line 8 to Page 23, line 11; and Page 29, lines 8-22; selecting keys using the key designation information).

Regarding Claim 7,

Nakano as modified by Lao discloses the server of claim 6, in addition, Nakano discloses that the key selection information storage unit further holds a plurality of key selection identifiers that identify the key selection information, the key selection identifiers and the key selection information being associated with each other (Figure 16; and Page 51, line 23 to Page 52, line 7; showing the format of key designation information including a node ID);

The encryption key group selection unit selects the selected node encryption key group based on the key selection information (Page 22, line 8 to Page 23, line 11; and Page 29, lines 8-22); and

The transmission unit distributes, to the content output apparatuses, the encrypted content, the encrypted content key decryption key, and the key selection identifiers associated with the key selection information (Page 74, line 23 to Page 75, line 14; showing transmission of encrypted content, encrypted content key, and key designation information).

Regarding Claim 8,

Nakano as modified by Lao discloses the server of claim 6, in addition, Nakano discloses that the encryption key group selection unit selects, on a random basis, one of the key selection information from among the plurality of key selection information held in the key selection

information storage unit, and selects the selected node encryption key group based on the selected key selection information (Page 22, line 8 to Page 23, line 11; the arbitrary setting of two or more terminal groups, as well as the selection of keys for each terminal and each terminal group. This all appears to be performed in a non-structured (e.g. random) basis, as groups can overlap and multiple groups can contain the same device, therefore, the groups must be selected "on a random basis". Further randomness is found in checking for keys corresponding to invalid terminals, such invalid terminals being randomly distributed throughout the terminals and/or groups).

Regarding Claim 9,

Nakano as modified by Lao discloses the server of claim 6, in addition, Nakano discloses that the key group selection unit selects, at regular intervals, one of the key selection information from among the plurality of key selection information held in the key selection information storage unit, and selects the selected node encryption key group based on the selected key selection information (Page 22, line 8 to Page 23, line 11; Page 48, line 24 to Page 49, line 3; and Page 51, lines 9-13; showing selecting the key groups; such selection being done at regular intervals. In this case, the interval is between distribution of each piece of content, when the key groups are selected, for example).

Regarding Claim 10,

Nakano as modified by Lao discloses the server of claim 1, in addition, Nakano discloses a storage unit operable to store the node encryption key group received via the network into the key information storage unit (Page 29, lines 8-22; storing key groups that have been received from the key setting system).

5. Claims 17-26, 30, 31, and 35-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakano in view of Asano (U.S. Patent Application Publication 2003/0051151).

Regarding Claim 17,

Nakano discloses a content output apparatus that receives an encrypted content from a content distribution server via a network, decrypts the encrypted content using a content decryption key, and outputs the decrypted content, the apparatus (decryption device) comprising:

A first receiving unit operable to receive the encrypted content and an encrypted content decryption key group which are distributed from the content distribution server (Page 31, lines 3-9; and Page 74, line 23 to Page 75, line 14; showing an obtaining unit receiving at least encrypted content and an encrypted content key);

A node key storage unit operable to hold the node decryption key group (Page 31, lines 10-15);

A decryption key obtaining unit operable to obtain the content decryption key based on at least one node decryption key group and at least one encrypted content decryption key group (Page 31, lines 22-26; key decryption unit decrypting the content key based on the selected decryption key); and

A first decryption unit operable to decrypt the encrypted content using the content decryption key (Page 31, line 27 to Page 32, line 3; decrypting the content using the content key);

But does not explicitly disclose a second receiving unit operable to receive, via the network, a node decryption key group which is previously assigned by a predetermined key assignment method.

Asano, however, discloses a second receiving unit operable to receive, via the network, a node decryption key group which is previously assigned by a predetermined key assignment method (Paragraphs 181-183; updating of keys in a key tree, and transmission of the updated keys to devices via a network; such second receiving unit being that which receives this transmission on the devices). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the key updating techniques of Asano into the data protection system of Nakano in order to allow the system to dynamically update key groups when desired, thereby forcefully removing invalid devices from the system by halting storage and usage of any of the keys held by such

invalid devices, thereby providing for forward secrecy, while allowing for periodic key updates such that, even if various keys used in the system are hacked, they will not be usable after such update, thereby further securing the system.

Regarding Claim 30,

Claim 30 is a program claim that corresponds to apparatus claim 17 and is rejected for the same reasons.

Regarding Claim 35,

Claim 35 is a method claim that corresponds to apparatus claim 17 and is rejected for the same reasons.

Regarding Claim 37,

Claim 37 is a computer readable recording medium claim that corresponds to apparatus claim 17 and is rejected for the same reasons.

Regarding Claim 18,

Nakano as modified by Asano discloses the apparatus of claim 17, in addition, Nakano discloses a key selection information storage unit operable to hold a plurality of key selection information of the node decryption keys in the node decryption key group and a plurality of key selection identifiers that identify the key selection information, the key selection information and the key selection identifiers being associated with each other (Figure 16; and Page 31, lines 3-21; reception, storage,

and usage of key designation information, including node identifiers, in selecting the key that is to be used);

Wherein the first receiving unit further receives the key selection identifiers (Figure 16; and Page 31, lines 3-21).

Regarding Claim 19,

Nakano as modified by Asano discloses the apparatus of claim 18, in addition, Nakano discloses that the decryption key obtaining unit obtains the content decryption key using the plurality of key selection information, based on the node decryption key group, the encrypted content decryption key group, and the key selection identifier (Figure 16; Page 31, lines 3-26; and Page 51, lines 9-13; obtaining and decrypting a content key from the encrypted content key group (e.g. keys 0-1K1000, 1-1K1000, and 2-1K1000 on page 51) based on the key selected from the node decryption key group above using key designation information including a node identifier).

Regarding Claim 20,

Nakano as modified by Asano discloses the apparatus of claim 17, in addition, Asano discloses a third receiving unit operable to receive key update information (Paragraphs 181-183); an individual key storage unit operable to hold a previously given individual key (Paragraph 176); and a second decryption unit operable to decrypt the key update information received based on the individual key, and store the decrypted node

decryption key group obtained by the decryption into the node key storage unit (Paragraphs 184-185; decrypting the updated keys with the device's leaf key (K0010), for example); and Nakano discloses that the decryption key obtaining unit obtains the content decryption key based on the node decryption key group and the encrypted content decryption key group (Page 31, lines 22-26); and the first decryption unit decrypts the encrypted content using the content decryption key (Page 31, line 27 to Page 32, line).

Regarding Claim 21,

Nakano discloses a key issuing center that is connected, via a network, with a content distribution server and content output apparatuses, and issues a key for obtaining a content decryption key to each of the content output apparatuses, the content distribution server distributing an encrypted content to the content output apparatuses, each of which receives the encrypted content, decrypts the received content using the content decryption key and outputs the decrypted content, the key issuing center (key setting system) comprising:

A node key generation unit operable to generate, based on a predetermined key assignment method, a node encryption key group that is a set of node encryption keys and a node decryption key group that is a set of node decryption keys, each of the node encryption keys and node decryption keys being assigned to each content output apparatus (Page

33, lines 7-17; Page 34, lines 4-16; and Page 38, lines 10-15; generation of key information for each node, the key information comprising at least a node encryption key and a node decryption key; and determining a set of keys per node);

A first transmission unit operable to transmit the node encryption key group to the content distribution server (Page 34, line 17 to Page 35, line 4);

A node decryption key group selection unit operable to select at least one of the node decryption keys, and generate the node decryption key group to be distributed to each content output apparatus (Page 34, lines 4-16; selecting a set of decryption keys for each device); and

A transmission unit operable to distribute the node decryption key group to a manufacturing system for storage in the content output apparatus (Page 34, lines 4-16);

But does not explicitly disclose a second transmission unit operable to distribute the node decryption key group to the content output apparatus itself.

Asano, however, discloses a second transmission unit operable to distribute the node decryption key group to the content output apparatus (Paragraphs 181-183; distributing the new keys to the devices). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the key updating techniques of Asano

into the data protection system of Nakano in order to allow the system to dynamically update key groups when desired, thereby forcefully removing invalid devices from the system by halting storage and usage of any of the keys held by such invalid devices, thereby providing for forward secrecy, while allowing for periodic key updates such that, even if various keys used in the system are hacked, they will not be usable after such update, thereby further securing the system.

Regarding Claim 31,

Claim 31 is a program claim that corresponds to key issuing center claim 21 and is rejected for the same reasons.

Regarding Claim 36,

Claim 36 is a method claim that corresponds to key issuing center claim 21 and is rejected for the same reasons.

Regarding Claim 38,

Claim 38 is a computer readable recording medium claim that corresponds to key issuing center claim 21 and is rejected for the same reasons.

Regarding Claim 22,

Nakano as modified by Asano discloses the center of claim 21, in addition, Nakano discloses a content output apparatus correspondence information storage unit operable to hold correspondence information between the generated plurality of node decryption key groups and the

plurality of content output apparatuses (Figure 9; Page 33, lines 4-6; and Page 40, lines 6-26; key information storage unit storing keys and information with respect to node IDs); and Asano discloses that the second transmission unit distributes the node decryption key groups to the content output apparatuses based on the correspondence information (Paragraphs 181-183).

Regarding Claim 23,

Nakano as modified by Asano discloses the center of claim 21, in addition, Nakano discloses that the key assignment method has a tree structure in which a plurality of content output apparatuses serve as nodes, and includes:

Classifying the nodes into a plurality of levels from a 0^{th} level to a nth level (n is 1 or a larger natural number) (Figure 4; and Page 33, lines 7-17);

Selecting a terminal node in the tree structure, the terminal node being (i) a node that belongs to the nth level or (ii) a node that belongs to the jth level (j is a natural number from 1 to n-1) and is not connected by lines with any nodes belonging to the j+1th level through the nth level (Figure 4; Page 33, lines 7-17; and Page 35, line 26 to Page 36, line 3); and

The node decryption key selection unit selects the selected node decryption key group so that the selected node encryption key group

includes at least a node encryption key that is set for a terminal node and a node encryption key that is set for a node other than the terminal node (Figures 4 and 8; and Page 33, lines 7-17).

Regarding Claim 24,

Nakano as modified by Asano discloses the center of claim 22, in addition, Asano discloses a first encryption unit operable to encrypt the node decryption key group selected by the node decryption key selection unit based on an individual key which is previously given to each content output apparatus, and generate an encrypted node decryption key group (Paragraphs 181-185); and

A key update information generation unit operable to generate key update information based on the encryption performed by the first encryption unit (Paragraphs 181-183);

Wherein the content output apparatus correspondence information storage unit further holds the individual key (Paragraphs 180 and 185; key K0010, for example, corresponding to the key 3-1K specific to the device in Nakano); and

The second transmission unit distributes the key update information to the content output apparatuses (Paragraphs 181-183).

Regarding Claim 25,

Nakano as modified by Asano discloses the center of claim 24, in addition, Nakano discloses that the content output apparatus

correspondence information storage unit further holds correspondence information between the output apparatus identifiers assigned to the content output apparatuses and the node decryption key groups (Figure 9; Page 33, lines 4-6; and Page 40, lines 6-26); and the node key generation unit generates the node encryption key group and the node decryption key group based on the key assignment method, in the case of receiving the node key generation request (Page 33, lines 7-17); and Asano discloses a correspondence information update unit operable to update the correspondence information held in the content output apparatus correspondence information storage unit based on a content output apparatus identifier, and output a node key generation request to the node key generation unit, the in the case of receiving a content output apparatus identifier from outside via the network (Paragraphs 181-183; in updating the keys, the center will update the correspondence between the keys and device(s)).

Regarding Claim 26,

Nakano as modified by Asano discloses the center of claim 24, in addition, Asano discloses that the node key generation unit outputs a key update information generation request to the first encryption unit, in the case of generating the node encryption key group and the node decryption key group based on the key assignment method (Paragraphs 181-183);

The first encryption unit encrypts the node decryption key group which is assigned to each content output apparatus using the previously given individual key, in the case of receiving the key update information generation request (Paragraphs 181-185); and

The key update information generation unit generates the key update information (Paragraphs 181-185).

6. Claims 27 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakano in view of Lao and Asano.

Regarding Claim 27,

Nakano discloses a content distribution system comprising content output apparatuses, and a content distribution server, each of the content output apparatuses decrypting an encrypted content using a content decryption key and outputting the decrypted content, and a content distribution server creating an encrypted content by encrypting the content, and distributing the encrypted content to each content output apparatus via a network:

Wherein the content output apparatus includes:

A first receiving unit operable to receive the encrypted content and an encrypted content decryption key group which are distributed from the content distribution server (Page 31, lines 3-9; and Page 74, line 23 to Page 75, line 14);

A node key storage unit operable to hold the node decryption key group (Page 31, lines 10-15);

A decryption key obtaining unit operable to obtain the content decryption key based on at least one node decryption key group and at least one encrypted content decryption key group (Page 31, lines 22-26); and

A first decryption unit operable to decrypt the encrypted content using the content decryption key (Page 31, line 27 to Page 32, line 3); and

The content distribution server includes:

A key information storage unit operable to hold a node encryption key group that is a set of node encryption keys which are previously assigned to the content output apparatuses using a predetermined key assignment method (Page 29, lines 8-22);

An encryption key group selection unit operable to select, from among the node encryption key group, at least one node encryption key as a selected node encryption key group (Page 22, line 8 to Page 23, line 11);

A content decryption key selection unit operable to generate an encrypted content decryption key group that includes at least one encrypted content decryption key obtained by encrypting a previously given content decryption key using the at least one node encryption key in the selected node encryption key group (Page 29, lines 4-7 and 23-27);

An encryption unit operable to encrypt the content using a content encryption key which is previously given as a pair with the content decryption key (Page 29, line 28 to Page 30, line 3); and

A transmission unit operable to distribute the encrypted content and the encrypted content decryption key group to the content output apparatuses (Page 30, lines 4-10; and Page 74, line 23 to Page 75, line 14);

But does not explicitly disclose a content receiving unit operable to receive a content via the network; or a second receiving unit operable to receive, via the network, a node decryption key group which is previously assigned by a predetermined key assignment method.

Lao, however, discloses a content receiving unit operable to receive a content via the network (Figure 7; Column 1, lines 8-12; Column 6, lines 31-36; Column 7, lines 63-67; and Column 9, lines 61-67). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the content publishing system of Lao into the data protection system of Nakano in order to allow the creators of content to specify the rights that may be allowed for a particular piece of content before allowing the content to be distributed, thereby ensuring proper control for content creators.

Asano, however, discloses a second receiving unit operable to receive, via the network, a node decryption key group which is previously

assigned by a predetermined key assignment method (Paragraphs 181-183). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the key updating techniques of Asano into the data protection system of Nakano as modified by Lao in order to allow the system to dynamically update key groups when desired, thereby forcefully removing invalid devices from the system by halting storage and usage of any of the keys held by such invalid devices, thereby providing for forward secrecy, while allowing for periodic key updates such that, even if various keys used in the system are hacked, they will not be usable after such update, thereby further securing the system.

Regarding Claim 28,

Nakano as modified by Lao and Asano discloses the system of claim 27, in addition, Asano discloses a key issuing center that is connected, via a network, with the content distribution server and the content output apparatuses, and issues a key for obtaining a content decryption key to each of the content output apparatuses, wherein the key issuing center includes:

A node key generation unit operable to generate, based on a predetermined key assignment method, a node encryption key group that is a set of node encryption keys and a node decryption key group that is a set of node decryption keys, each of the node encryption keys and node

decryption keys being assigned to each content output apparatus (Page 33, lines 7-17; Page 34, lines 4-16; and Page 38, lines 10-15);

A first transmission unit operable to transmit the node encryption key group to the content distribution server (Page 34, line 17 to Page 35, line 4);

A node decryption key group selection unit operable to select at least one of the node decryption keys, and generate the node decryption key group to be distributed to each content output apparatus (Page 34, lines 4-16); and

A transmission unit operable to distribute the node decryption key group to a manufacturing system for storage in the content output apparatus (Page 34, lines 4-16); and

Asano discloses a second transmission unit operable to distribute the node decryption key group to the content output apparatus (Paragraphs 181-183).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2437

/Jeffrey D Popham/
Examiner, Art Unit 2437